Notice of Allowability	Application No.	Applicant(s)	
	09/763,621	VATER ET AL.	
	Examiner	Art Unit	
	CARL COLIN	2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed on 3/27/2009 and interview held on 6/1/2009*.

2. ☒ The allowed claim(s) is/are *1-3, 5-11 and 13-18*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *held on 6/1/2009* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Carl Colin/
Primary Examiner, Art Unit 2433

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/27/2009 has been entered.

Response to Arguments

2. In response to communications filed on 3/27/2009, Applicant amends claims 1-3, 5, 6, 9-11, and 13-15; and cancels claims 4 and 12. Claims 1-3, 5-11, and 13-18 are presented for examination.

3. Applicant's arguments see pages 7-11, filed on 3/27/2009, with respect to the rejection of claims 1-18 have been fully considered, and they are persuasive as amended.

EXAMINER'S AMENDMENT

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Applicant's attorney on June 1 2009 and June 5, 2009.

The application has been amended as follows:

Amendment to the Specification is as follows:

The paragraph bridging pages 4 and 5:

Figure 3b shows an intermediate step in determining the disguised lookup table of Figure 3c. The lookup table according to Figure 3b was generated from the lookup table according to Figure 3a by XORing each value of the first line of the table from Figure 3a with random number R_1 = 11. Thus, XORing the value 00 of the first line and first column of the table from Figure 3a with the number 11 yields the value 11, which is now the element of the first line and first column of the table of Figure 3b. The remaining values of the first line of the table shown in Figure 3b are determined accordingly from the values of the first line of the table shown in Figure 3b are determined accordingly from the values of the first line of the bale shown in Figure 3a and random number R_1 = 11. Basically, the XOR function changes 00, 01, 10, and 11 of Fig. 3A to 11, 10, 01, 00. Since h(x) as shown in Fig. 3A maps 00 to 01, 01 to 11, 10 to 10, and 11to 00, the result of disguising the input data would be to map 11 to 00, 10 to 10, 01 to 11, and 00 to 01. However, as shown in Fig. 3B, as a result of the disguised input data x, the operation is also disguised to become the disguised operation $h_{R1}(x)$, so that 11 now maps to 01, 10 to 11, 01 to 10 and 00 to 00. The result is that the second line of Fig. 3B is exactly the same as the second line of Fig. 3A, but that the input data is disguised and the operation, in the form of a mapping, is also disguised. ~~The~~ Thus, table shown in Figure 3b could already be used as a disguised lookup table

for processing secret data likewise disguised with random number $R_1 = 11$. The result would be the plaintext values to be read in line 2 of this table from Figure 3b.

Page 5, lines 14-16:

If the table according to Figure 3c, which preserves the mapping or disguised input data and disguised operation of Fig. 3b, is to be disguised further or yield as output values likewise disguised values rather than plaintext values, one applies a further XOR operation with further random number R_2.

Page 2, lines 12-15:

The security-relevant operation will be represented in the following by function h mapping input data x on output data y, i.e. $y = h(x)$. To prevent secret input data x from being spied out the invention provides, in one example, for a disguised function h_{R1} to be determined, so that the following holds:

$$h(x) = h_{R1}(x \otimes R_1)$$

as shown in Figs.3a-3c, or in a variation of the basic disguising operation, for disguised function h_{R1R2} to be determined, so that the following holds:

$$y \otimes R_2 = h_{R1R2}(x \otimes R_1),$$

as shown in Fig. 3d.

Amendment to the Claims is as follows:

In claim 13, on the first line, replace "12" by --9--.

Allowable Subject Matter

5. Claims 1-3, 5-11, and 13-18 are allowed.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2433
June 11, 2009